

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-312364

(43) 公開日 平成11年(1999)11月9日

(51) Int. Cl. ⁶

識別記号

F I

G11B 20/10

G11B 20/10

H

H04N 5/765

H04N 5/781

510

L

5/781

5/92

H

5/92

7/13

Z

7/24

審査請求 未請求 請求項の数12 O L (全11頁)

(21) 出願番号

特願平10-118924

(22) 出願日

平成10年(1998)4月28日

(71) 出願人 000006013 -

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 勢木 真一

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

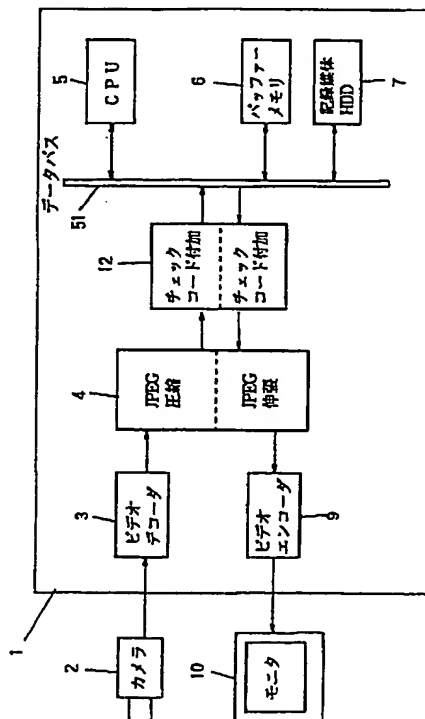
(74) 代理人 弁理士 前田 実

(54) 【発明の名称】 デジタルデータ記録装置、デジタルデータ再生装置、及びチェックコード生成方法

(57) 【要約】

【課題】 媒体に記録されているデジタルデータが改変されたものかどうかを容易に検出できるデジタルデータ記録／再生装置を提供する。

【解決手段】 カメラ2から入力された映像はビデオデコーダ3によりデジタル映像データに変換され、JPEG圧縮伸張手段4でJPEGデータに圧縮される。このJPEGデータから、チェックコード付加解析器12によってJPEGデータからサンプリングし、10点のサンプリングデータを得さらに、このサンプリングデータに演算を加え、チェックコードを生成しJPEGデータのヘッダー内に付加する。このようにして生成したチェックコード付のJPEGデータを記録媒体7に記録する。その後、何者かが、記録された映像データの改変しても再生時に高い精度で改変の有無を検出できる。



【特許請求の範囲】

【請求項 1】 デジタルデータを記録媒体に記録するデジタルデータ記録装置において、デジタルデータを圧縮するデータ圧縮手段と、圧縮されたデジタルデータから一部のデータを第 1 の暗号関数に基づいて抽出する抽出手段と、抽出されたデータを変数として第 2 の暗号関数に基づいてチェックコードを生成する生成手段と、前記チェックコードを前記圧縮されたデジタルデータの所定位置に付加する付加手段とを備えたことを特徴とするデジタルデータ記録装置。

【請求項 2】 前記第 2 の暗号関数は、サンプリング番号を変数とした暗証番号を変数とすることを特徴とする請求項 1 に記載のデジタルデータ記録装置。

【請求項 3】 前記デジタルデータがデジタル画像データであって、このデジタル画像データを圧縮する J P E G 圧縮手段を備え、前記チェックコードを J P E G 圧縮データのヘッダー内に付加したことを特徴とする請求項 1 または請求項 2 に記載のデジタルデータ記録装置。

【請求項 4】 記録媒体に圧縮して記録されたデジタルデータを再生するデジタルデータ再生装置において、圧縮デジタルデータから一部のデータを第 1 の暗号関数に基づいて抽出する第 1 の抽出手段と、前記第 1 の抽出手段で抽出されたデータを変数として第 2 の暗号関数に基づいて第 1 のチェックコードを生成する生成手段と、圧縮デジタルデータに付加されている第 2 のチェックコードを抽出する第 2 の抽出手段と、前記第 1 のチェックコードと前記第 2 のチェックコードとを比較する比較手段と、前記圧縮デジタルデータを伸張する伸張手段とを備えたことを特徴とするデジタルデータ再生装置。

【請求項 5】 記録媒体に圧縮して記録されたデジタルデータを再生するデジタルデータ再生装置において、圧縮デジタルデータから一部のデータを第 1 の暗号関数に基づいて抽出する第 1 の抽出手段と、圧縮デジタルデータに付加されているチェックコードを抽出する第 2 の抽出手段と、前記第 1 の抽出手段で抽出されたデータと前記チェックコードとを第 3 の暗号関数に基づいて演算する演算手段と、前記圧縮デジタルデータを伸張する伸張手段とを備えたことを特徴とするデジタルデータ再生装置。

【請求項 6】 前記デジタルデータがデジタル画像データであって、

圧縮されたデジタル画像データを伸張する J P E G 伸

張手段を備え、

前記チェックコードを J P E G 圧縮データのヘッダーから抽出したことを特徴とする請求項 4 または請求項 5 に記載のデジタルデータ再生装置。

【請求項 7】 請求項 1 乃至請求項 3 のいずれかのデジタルデータ記録装置、或いは請求項 4 乃至請求項 6 のいずれかのデジタルデータ再生装置に使用されるチェックコードの生成方法であって、圧縮されたデジタルデータの中から複数のサンプリングデータを抽出し、

前記抽出されたサンプリングデータとそのサンプリング番号を変数とした暗証番号とを変数としてチェックコードを生成することを特徴とするチェックコード生成方法。

【請求項 8】 前記サンプリング番号を変数とした暗証番号は、暗号関数に基づいて生成されていることを特徴とする請求項 7 に記載のチェックコード生成方法。

【請求項 9】 前記チェックコードは、抽出されたサンプリングデータと前記暗証番号とを変数とする算術加算関数によって生成されていることを特徴とする請求項 7 に記載のチェックコード生成方法。

【請求項 10】 前記チェックコードは、抽出されたサンプリングデータと前記暗証番号とを変数とするガロア体上での加算によって生成されていることを特徴とする請求項 7 に記載のチェックコード生成方法。

【請求項 11】 前記チェックコードは、抽出されたサンプリングデータと前記暗証番号とを変数とする排他的論理和演算によって生成されていることを特徴とする請求項 7 に記載のチェックコード生成方法。

【請求項 12】 前記サンプリングデータは、圧縮されたデジタルデータの中から暗号関数に基づいて抽出されていることを特徴とする請求項 7 乃至請求項 11 のいずれかに記載のチェックコード生成方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、圧縮されたデジタルデータを記録媒体に記録し、或いは記録媒体から再生するデジタルデータ記録／再生装置、及びデジタルデータ記録／再生装置のデジタル画像の改変を検出するためのチェックコードの生成方法に関する。

【0002】

【従来の技術】図 8 は、従来のデジタル画像記録再生装置の構成を示すブロック図である。1 はデジタル画像記録再生装置、2 はデジタル画像記録再生装置 1 に接続されたビデオカメラ、3 はビデオカメラ 2 からのアナログ映像信号をデジタル映像データに変換するビデオデコード、4 は J P E G 圧縮伸張手段、5 はこのデジタル画像記録再生装置 1 の制御を行う C P U、5 1 は C P U 5 のデータバス、6 はデータバス 5 1 に接続され J P E G 圧縮伸張手段 4 で圧縮された J P E G データの

一時的格納などに用いるバッファメモリ、7はJ P E Gデータを保存するためのH D D等の記録メディア、9は4 : 2 : 2プロファイルのデジタル映像データ

(Y、C R、C Bのデータ量が4 : 2 : 2のデジタル映像データ) をN T S Cアナログ信号に変換するビデオエンコーダ、11はデジタル画像記録再生装置1に接続されたモニタテレビである。

【0003】つぎに、このデジタル画像記録再生装置で圧縮されたデジタルデータを記録媒体に記録し、或いは記録媒体から再生する動作について説明する。

【0004】図9は、記録時の信号処理の流れを示すフローチャートである。処理ステップS T 2 0において、ビデオカメラ2で撮影されたアナログ映像信号はデジタル画像記録再生装置1に入力され、ビデオデコーダ3によって4 : 2 : 2のデジタル映像データに変換される。次の処理ステップS T 2 1では、J P E G圧縮伸張手段4によってJ P E Gデータに圧縮される。処理ステップS T 2 2においては、J P E Gデータはデータバス51を通して一旦バッファメモリ6に格納され、バッファメモリ6の中でタイムデートコード等を含んだヘッダーがJ P E Gデータに付加される。さらに処理ステップS T 2 3において、ヘッダーが付加されたJ P E Gデータはデータバス51を通して記録メディア7に記録される。

【0005】図10は、再生時の信号処理の流れを示すフローチャートであって、処理ステップS T 3 0において、記録メディア7に記録されたJ P E GデータはC P U 5の制御によって一旦バッファメモリ6に格納される。次に、処理ステップS T 3 1ではヘッダー情報を抽出し、これによって時刻表示のデータなどを生成する。処理ステップS T 3 2において、J P E Gデータはデータバス51を通してJ P E G圧縮伸張手段4に送られ、4 : 2 : 2デジタル映像データに伸張される。最後に処理ステップS T 3 3において、伸張された4 : 2 : 2デジタル映像データをビデオエンコーダ9によってN T S Cアナログ信号に変換し、モニタテレビ10により再生映像を表示する。

【0006】

【発明が解決しようとする課題】上記デジタル画像記録再生装置1は、間欠記録の可能なデジタルタイムラプスレコーダとして鉄道、空港などの交通機関や、銀行など金融機関で、或いは化学実験や動植物の観察等の学術研究用途に広く用いられている。そこでは、記録された映像データを解析するため、記録の際にJ P E G圧縮されたデータを外部に出力するS C S IインターフェースやR S 2 3 2 C端子を備えた装置が使用され、圧縮データをパソコンなどに送り、このパソコン等でJ P E G伸張することで通常の画像データに変換することができる。したがって記録された映像データは、コンピュータの画像処理ソフト等を用いて、コントラストの調整や輪

郭強調や部分拡大などの修正を行うことができ、その後再びJ P E G圧縮して保存することも可能である。

【0007】しかし、修正された映像データと同じデジタル画像記録再生装置1に記録した場合、どれが元の記録データで、どれが修正後のデータなのか分からなくなってしまう恐れがあった。

【0008】また、悪意を持った第三者が同様の方法で元の記録データを加工し、あるいは他のデータと入れ替えることが可能であるため、そのような画像データの一部が改変されたことを容易には検出することができなかった。これは、上記デジタル画像記録再生装置1により記録された、犯罪などの証拠となり得る映像データを何者かが改変したり、あるいは犯罪の証拠となる映像データに対して部分的な追加や削除等が行われても、そのデータ自体からはデータの改変は検出できないことを意味する。このためデジタル映像データの証拠能力については、犯罪などを立証するに足りるものとは看做されていなかった。

【0009】さらに、オリジナルデータであるか否かを確認するには、暗号技術を応用した方法がある。ところが、このような方法を動画像データに適用しようとする、膨大で複雑な計算が必要となりコストの高いものになる問題がある。単純な確認方法としては、誤りの存在を検査するために使用されるチェックサム (Checksum) をチェックデータとして映像データに付加することも考えられる。しかし、加算によって付加されたチェックデータは容易に解読されてしまううえ、動画像データの場合にはチェックサムを付加するだけでもデータ処理量が多くなるため、専用のハードウェアを設ける必要があるという問題もあった。

【0010】この発明は上記のような問題を解決するためのものであり、媒体に記録されているデジタルデータが改変されたものかどうかを容易に検出できるデジタルデータ記録／再生装置を提供することを目的としている。

【0011】また、記録媒体に記録されている画像データが改変されたものであるかどうかを容易に検出でき、しかも解読のされにくいチェックコード生成方法を提供するものである。

【0012】

【課題を解決するための手段】請求項1に係るデジタルデータ記録装置は、デジタルデータを記録媒体に記録するデジタルデータ記録装置において、デジタルデータを圧縮するデータ圧縮手段と、圧縮されたデジタルデータから一部のデータを第1の暗号関数に基づいて抽出する抽出手段と、抽出されたデータを変数として第2の暗号関数に基づいてチェックコードを生成する生成手段と、チェックコードを圧縮されたデジタルデータの所定位置に付加する付加手段とを備えたものである。

【0013】請求項2に係るデジタルデータ記録装置では、第2の暗号関数は、サンプリング番号を変数とした暗証番号を変数とするものである。

【0014】請求項3に係るデジタルデータ記録装置は、デジタルデータがデジタル画像データであって、このデジタル画像データを圧縮するJ P E G圧縮手段を備え、チェックコードをJ P E G圧縮データのヘッダー内に付加したものである。

【0015】請求項4に係るデジタルデータ再生装置は、記録媒体に圧縮して記録されたデジタルデータを再生するデジタルデータ再生装置において、圧縮デジタルデータから一部のデータを第1の暗号関数に基づいて抽出する第1の抽出手段と、第1の抽出手段で抽出されたデータを変数として第2の暗号関数に基づいて第1のチェックコードを生成する生成手段と、圧縮デジタルデータに付加されている第2のチェックコードを抽出する第2の抽出手段と、第1のチェックコードと第2のチェックコードとを比較する比較手段と、圧縮デジタルデータを伸張する伸張手段とを備えたものである。

【0016】請求項5に係るデジタルデータ再生装置は、記録媒体に圧縮して記録されたデジタルデータを再生するデジタルデータ再生装置において、圧縮デジタルデータから一部のデータを第1の暗号関数に基づいて抽出する第1の抽出手段と、圧縮デジタルデータに付加されているチェックコードを抽出する第2の抽出手段と、第1の抽出手段で抽出されたデータとチェックコードとを第3の暗号関数に基づいて演算する演算手段と、圧縮デジタルデータを伸張する伸張手段とを備えたものである。

【0017】請求項6に係るデジタルデータ再生装置は、デジタルデータがデジタル画像データであって、圧縮されたデジタル画像データを伸張するJ P E G伸張手段を備え、チェックコードをJ P E G圧縮データのヘッダーから抽出したものである。

【0018】請求項7に係るチェックコード生成方法は、デジタルデータ記録装置、或いはデジタルデータ再生装置に使用されるチェックコードの生成方法であって、圧縮されたデジタルデータの中から複数のサンプリングデータを抽出し、抽出されたサンプリングデータとそのサンプリング番号を変数とした暗証番号とを変数としてチェックコードを生成するものである。

【0019】請求項8に係るチェックコード生成方法では、サンプリング番号を変数とした暗証番号は、暗号関数に基づいて生成されている。

【0020】請求項9に係るチェックコード生成方法では、チェックコードは、抽出されたサンプリングデータと暗証番号とを変数とする算術加算関数によって生成されている。

【0021】請求項10に係るチェックコード生成方法では、チェックコードは、抽出されたサンプリングデー

タと暗証番号とを変数とするガロア体上での加算によって生成されている。

【0022】請求項11に係るチェックコード生成方法では、チェックコードは、抽出されたサンプリングデータと暗証番号とを変数とする排他的論理和演算によって生成されている。

【0023】請求項12に係るチェックコード生成方法では、サンプリングデータは、圧縮されたデジタルデータの中から暗号関数に基づいて抽出されている。

【0024】

【発明の実施の形態】実施の形態1. 図1は、この発明の実施の形態1におけるデジタル画像記録再生装置の構成を示すブロック図である。従来例の対応する図面(図8)と対応する部分には同一の符号を付けている。

【0025】図において、1はデジタル画像記録再生装置、2はデジタル画像記録再生装置1に接続されたビデオカメラ、3はビデオカメラ2からのアナログ映像信号を4:2:2プロファイルのデジタル映像データに変換するビデオデコーダ、4はJ P E G圧縮伸張手段、12はJ P E G圧縮データに対して固有のチェックコードを付加し、解析するチェックコード付加解析器、5はこのデジタル画像記録再生装置1の制御を行うC P U、51はC P U 5のデータバス、6はデータバス51に接続されJ P E G圧縮伸張手段4で圧縮されたJ P E Gデータの一時的格納などに用いるバッファメモリ、7はJ P E Gデータを保存するためのH D D等の記録メディア、9は4:2:2プロファイルのデジタル映像データをN T S Cアナログ信号に変換するビデオエンコーダ、10はデジタル画像記録再生装置1に接続されたモニタテレビである。

【0026】図2は、記録時の信号処理の流れを示すフローチャートであって、処理ステップS T 20~23は図9の各処理に対応するものである。処理ステップS T 20においてビデオカメラ2で撮影されたアナログ映像信号はデジタル画像記録再生装置1に入力されビデオデコーダ3によって4:2:2のデジタル映像データに変換される。次に、処理ステップS T 21ではJ P E G圧縮伸張手段4によってJ P E Gデータに圧縮される。処理ステップS T 40においてサンプリングされたJ P E Gデータは、処理ステップS T 41においてチェックコード付加解析器12による演算で所定のチェックコードが生成される。このチェックコードは、処理ステップS T 21で圧縮されたJ P E Gデータと共にデータバス51を通過して一旦バッファメモリ6に格納される。

【0027】次に、処理ステップS T 41におけるチェックコードの生成方法について述べる。まず、処理ステップS T 40においてJ P E GデータD (i)の中から、各1バイトのサンプリングデータとして、例えば10点(n=0~9)を選んで各1バイトのサンプリング

データ $S(n)$ を第 1 の暗号関数、例えば以下の式
(1) に基づいて抽出する。

$$S(n) = D(a \times n + b) \quad \dots (1)$$

ただし、 n はサンプリング番号、 a 、 b は定数である。

【0029】処理ステップ ST 4 1 では、これらのサンプリングデータ $S(0) \sim S(9)$ を変数として、次式
(2) に示される暗号関数 ($F(*)$) : 第 2 の暗号関

$$C(n) = F(S(n), X(n)) \quad \dots (2)$$

なお、 $X(n)$ は暗証番号配列を決定するための暗号関数である。

【0031】この $F(*)$ の演算はチェックコードのルールを他者に解析されにくくするためのもので、この秘密とされる暗号関数 $F(*)$ だけでなく、暗証番号配列を決定する暗号関数 $X(n)$ 、及び上記定数 a 、 b をも秘密にしておけば、チェックコード $C(n)$ の解析は非常に困難になる。

【0032】図 4 は、チェックコードの生成方法を模式的に示した図である。図において、610 は圧縮された

$$C(n) = S(n) + n$$

ただし、 n はサンプリング番号で 0 ~ 9 である。

【0035】処理ステップ ST 4 2 によってこのチェックコード 621 とタイムデートコード等を含んだヘッダーデータ 620 を生成し、処理ステップ ST 2 2 で上記 J P E G データ 610 に付加する。なお、このヘッダーデータ 620 は J P E G 規格に準拠した形で構成される。処理ステップ ST 2 3 において、このヘッダーデータ 620 が付加された J P E G データ 610 はデータバス 51 を通って記録メディア 7 に記録される。

【0036】次に、再生時の動作について説明する。図 3 は、再生時の信号処理の流れを示すフローチャートであって、処理ステップ ST 3 0 ~ 3 3 は図 10 の各処理に対応するものである。

【0037】処理ステップ ST 3 0 において記録メディア 7 に記録されている J P E G データは、CPU 5 の制御によって一旦バッファメモリ 6 に格納される。このバッファメモリ 6 に格納された J P E G データから処理ステップ ST 3 1 でヘッダー情報が抽出され、さらに処理ステップ ST 4 3 によってヘッダーからチェックコードが抽出される。

【0038】また、処理ステップ ST 3 1、4 3 に並行して、処理ステップ ST 4 0 においてバッファメモリ 6 に格納された J P E G データから記録時と同様の方法でチェックコードが生成される。すなわち、上記式

(1) によって J P E G データ $D(i)$ の中から記録時と同じ 10 点 ($n = 0 \sim 9$) のサンプリングデータ S

(n) を求める。処理ステップ ST 4 1 では、10 点のサンプリングデータ $S(n)$ に上記式 (3) に示される演算を施して、チェックコード $C(n)$ を生成する。この処理ステップ ST 4 1 での演算は、記録時に行われたチェックコードを求めるための演算と同一の処理であっ

【0028】

数) に基づいて演算を施し、チェックコード $C(n)$ を生成する。

【0030】

J P E G データ、620 はその先頭のタイムデートコード等を含んだヘッダーデータ、621 はヘッダー内に付加されたチェックコードである。

【0033】生成されるチェックコードの具体例としては、秘密の関数 $F(*)$ を算術加算、暗証番号配列を決定する $X(n) = n$ としたとき、式 (2) のチェックコード $C(n)$ を書き換えると、次の式 (3) になり、チェックコードの配列は図 5 のようになる。

【0034】

$$\dots (3)$$

て、通常は処理ステップ ST 4 3 で抽出したチェックコードと同一のものとなるが、記録後にデータの改変が行われているときは異なるチェックコードとして求められる。

【0039】その後、処理ステップ ST 4 5 において、処理ステップ ST 4 3 で抽出したチェックコードと処理ステップ ST 4 1 によって算出したチェックコードを比較する。もし、2 つのチェックコードが互いに異なっていた場合には、記録後にデータの改変が行われたものであるから、処理ステップ ST 4 6 によってモニタテレビ 10 に対して警告表示を出すように指令する。これにより、再生された映像データが一旦記録メディア 7 に格納された後に何者かによって改変を加えられた旨の警告がなされる。

【0040】処理ステップ ST 3 2 では、J P E G データがデータバス 51 を通って J P E G 圧縮伸張手段 4 に送られ、再びデジタル映像データに伸張される。この伸張されたデジタル映像データは、処理ステップ ST 3 3 において、ビデオエンコーダ 9 によって N T S C アナログ信号に変換され、モニタテレビ 10 に再生映像を表示する。処理ステップ ST 4 6 で指令された警告は、この時の再生映像の上に重ねて表示し、改ざんされたデータであることを明示する。こうして再生中の映像データが、何者かによって改ざんされたものであることを明らかにできる。

【0041】以上のように、圧縮された J P E G データの一部をサンプリングしてチェックコードを生成し、デジタル映像データとともに記録メディア 7 に格納するようにしたので、非常に少ないデータの処理量で記録されているデジタルデータが改変されたものかどうかを容易に検出することができる。

【0042】つぎに、何者かが記録された映像データを、一旦、J P E G伸張することで通常の画像データに変換して、その後にコンピュータの画像処理ソフト等を用いて画像データの一部を改変した後、再びJ P E G圧縮して元の記録データと入れ替えてしまうような場合について考察する。映像データを改変した範囲が映像データの一部に限られた領域だけであっても、J P E G圧縮処理の過程で行われるD C T符号化、あるいはハフマン符号化によって圧縮された後のJ P E Gデータでは、一部改変による元の映像データの影響が圧縮後のJ P E Gデータの全域に広がってしまう。このため、10点程度の少ないサンプリングポイントを使用するだけであっても、映像データの改変を確実に検出することができる。

【0043】また、改変した映像データに対して新たにチェックコードを付けて、改変したことを分からなくすることも不可能に近い。何故ならば、式(1)および式(2)で示された映像データからのサンプリングルールやチェックコードの演算方法は暗号関数に基づくものであり、暗証番号配列を決定するための暗号関数を含めて全ての暗号関数が知られていない限りでは、第三者がチェックコード自体を解析することは極めて困難だからである。したがって、この実施の形態1のデジタル画像記録再生装置は、映像データの証拠能力を高めるうえでも有効である。

【0044】以上述べたように、実施の形態1のデジタルデータ記録再生装置におけるデジタル画像の改変を検出するためのチェックコードの生成方法は、簡便な方法でありながら、非常に高い検出能力と、悪意を持った第三者による解析に対しても高い信頼性を持っている。このため犯罪などが発生した場合においても、本実施の形態のデジタルデータ記録装置で記録された映像データは高い証拠能力がある。

【0045】なお、チェックコードはJ P E G圧縮したヘッダーデータの未使用の予約領域に格納することで、通常のチェックコードを付加、解析する機能のないデジタルデータ記録再生装置であっても再生することが可能である。

【0046】実施の形態2、実施の形態1では、チェックコードCを生成する際の暗号関数F(*)として、式(2)に示すような通常の算術加算を用いたが、これは他の関数であっても良い。例えばガロア体(有限体)の加法演算などを用いて、チェックコードを生成することもできる。

【0047】実施の形態1では、8 b i tデータに対して通常の算術加算を行っているために加算結果に桁上がりが発生した場合に、演算結果が8 b i tデータでは収まらなり、桁上がり部分の切り捨てが行われる。このため、異なるサンプリングデータに対して同一のチェックコードを生成することになるが、そうすると映像データの改変を見逃してしまう可能性がある。そこで、暗号

関数F(*)として式(2)のような通常の算術加算の代わりにガロア体上の加算を用いることで、サンプリングデータが異なれば必ず異なるチェックコードが生成される。これによって、映像データの改変を見逃してしまう可能性を小さくすることができる。

【0048】実施の形態3、実施の形態1では、チェックコードC(n)を生成する際に、式(2)に示すような暗号関数F(*)として通常の算術加算を用いたが、これは他の関数であっても良く、例えば排他的論理和演算を用いてもよい。図6に示すように、ヘッダーデータ(上位)と暗証番号配列X(10)、ヘッダーデータ(下位)と暗証番号配列X(11)、サンプリングデータS(0)と暗証番号配列X(0)、等の間で排他的論理和演算を実行する。このような演算によれば、実施の形態2と同様に、サンプリングデータが異なれば必ず異なるチェックコードを生成することができる。

【0049】この方法は、実施の形態2で用いたガロア体の加算を用いる方法よりも簡単にチェックコードを生成できる効果がある。

【0050】また、図6に示すようにヘッダーデータとは別に暗号関数のバージョン情報をチェックコードに付加し、このバージョン情報に応じて映像データからのサンプリングルールやチェックコードの演算方法、及び暗証番号配列を決定するための暗号関数を変更することもできる。ここで、バージョン情報とはそれぞれ異なる暗号関数を記憶する複数のバージョン(Ver. 1.0、Ver. 2.0等)を特定する情報であって、装置毎に、あるいは記録期間毎に使用した暗号関数のバージョン情報がチェックコードに付加される。

【0051】こうすれば、あるバージョンの暗号関数が悪意を持った第三者に知られた場合でも、それ以外のバージョンの暗号関数で生成されたチェックコードの信頼性を保つことができ、画像データの改変を防止できる効果がある。

【0052】また、図4に示すヘッダー620を、例えば挿入されるチェックコード621よりも前の部分(上位部分)と後ろの部分(下位部分)とに分割し、上位部分のヘッダーを加算して上位のヘッダーデータとし、下位部分のヘッダーを加算して下位のヘッダーデータとする。これら上位、下位のヘッダーデータと暗証番号配列X(10)、X(11)との排他的論理和演算をおこなって、サンプリングデータから生成されたチェックコードに付加する。このようなチェックコードを用いることで、ヘッダー情報自体が改変された場合にもそれを検出することができる。ヘッダー部分には、J P E Gデータの伸張に必要な情報の他、日時情報やカメラ番号などの重要な情報が記録されているため、このようなヘッダー部分の改変の検出手段を設けることで、さらに信頼性の高い装置を得ることができる。

【0053】実施の形態4

実施の形態1～3では、秘密の関数 $F(*)$ として式(2)に示すように、1つのサンプリングデータと1つの暗証番号を用いて、一つのチェックコードを算出したが、以下の式(4)に示すように、複数のサンプリング

$$C(n) = F(S(n), S(n+1), X(n), X(n+1)) \dots (4)$$

この場合には、悪意を持った第三者によるチェックコードの解析をより一層困難なものにし、チェックコードの信頼性を上げる効果がある。

【0055】実施の形態5. 実施の形態1では、式

(1)に示す一次式で予め決められた定数 a 、 b を用い

$$S(n) = D((N+2)n/16) \dots (5)$$

となり、16分割されたデータのうちの3番目のデータから10点をサンプリングできる。こうすればサンプリングポイントの数は変わらないので、JPEGデータが小さい場合でも改変検出の精度が低くならない効果がある。また、JPEGデータのデータ量によってサンプリングポイントを容易に変更できるので、悪意を持った第三者によるチェックコードの解析をより一層困難なものにし、チェックコードの信頼性を上げる効果がある。

【0057】実施の形態6. 実施の形態1では、サンプリングデータ $S(n)$ をサンプリングする方法として、式(1)に示す一次式を用いたが、他の方法でサンプリングしても良い。例えば、対数、三角関数などの他の関数は、その例である。また、乱数を用いてサンプリングする方法や、秘密の暗証番号を用いてサンプリング位置を変えても良い。この場合、悪意を持った第三者によるチェックコードの解析をより一層困難なものにし、チェックコードの信頼性を上げる効果がある。

【0058】実施の形態7. 図7は、この発明の実施の形態7における再生時の信号処理の流れを示すフローチャートであって、処理ステップST30～33は図10

$$V(n) = S(n) - C(n) + n \dots (6)$$

のような演算を設定しておけば、処理ステップST48における演算結果 $V(n) = 0$ であるかどうかによって、改変の有無が判断できる。

【0062】したがって、処理ステップST48において $V(n) \neq 0$ であれば、処理ステップST46によってモニタテレビ10に対して警告表示を出すように指令して、何者かによって改変されたものであることを知らせることが可能になる。

【0063】なお、上記実施の形態1～7では、いずれも画像データの圧縮方法としてJPEG圧縮を用いているが、MPEG1、MPEG2、MPEG4、H.261など、他の圧縮方法による映像データに対しても同様に有効である。

【0064】また、記録装置として間欠記録を行うデジタルタイムラプスレコーダ以外に通常の連続記録装置にも適用でき、同様の効果を奏する。

【0065】また、上記実施の形態1～7では画像データの記録について説明したが、例えば音声データ等、他

データと複数の暗証番号を用いて、一つのチェックコードを算出してもよい。

【0054】

ていたが、JPEGデータのデータ量が変わってもサンプリングポイントの数 n が変わらないように、定数 a 、 b をデータ量に応じて変更するようにしてもよい。

【0056】例えば、 N を全データ数、 $a = N/16$ 、

$b = 2a$ のように決定しておけば、

の各処理に対応するものである。

【0059】処理ステップST30において記録メディア7に記録されているJPEGデータは、CPU5の制御によって一旦バッファメモリ6に格納される。このバッファメモリ6に格納されたJPEGデータから処理ステップST31でヘッダー情報が抽出され、さらに処理ステップST43によってヘッダーからチェックコードが抽出される。

【0060】また、処理ステップST31、43に並行して、処理ステップST40では、このバッファメモリ6に格納されたJPEGデータから式(1)によってサンプリングデータ $S(n)$ を求める。処理ステップST47では、このサンプリングデータ $S(n)$ と処理ステップST43によって抽出されたチェックコードとが直接に演算され、改変されたデータかどうかのチェックが行なわれる。

【0061】処理ステップST47における演算としては、例えば記録時のチェックコードが式(3)により生成されている場合には、

の種類のデータを記録再生するものであっても同様の効果を奏する。

【0066】さらに、上記実施の形態1～7ではチェックコードの付加解析器12に専用の回路を設けているが、これらの処理は非常に簡便に行うことができるので、CPU5によってソフトウェア的に実行するようにしてハードウェアを簡素化することも可能である。

【0067】

【発明の効果】この発明は、以上説明したように構成されているので、以下に示すような効果を奏する。

【0068】請求項1に記載したデジタルデータ記録装置によれば、媒体に記録されているデジタルデータが改変されたものかどうかを容易に検出できる。

【0069】請求項2の装置では、第2の暗号関数は、サンプリング番号を変数とした暗証番号を変数とするので、チェックコードの解析は非常に困難になり、映像データの証拠能力を高めるうえで有効である。

【0070】請求項3の装置では、デジタルデータが

デジタル画像データである場合に、このデジタル画像データを圧縮するＪＰＥＧ圧縮手段を備え、チェックコードをＪＰＥＧ圧縮データのヘッダー内に付加したので、デジタル画像の改変を簡便な方法で検出でき、悪意を持った第三者の改変を高い信頼性で防止できる。

【００７１】請求項４に記載したデジタルデータ再生装置によれば、再生されているデジタルデータが改変されたものかどうかを容易に検出できる。

【００７２】請求項５に記載したデジタルデータ再生装置によれば、簡単な演算だけで再生されているデジタルデータが改変されたものかどうかを容易に検出できる。

【００７３】請求項６の装置では、デジタルデータがデジタル画像データである場合に、圧縮されたデジタル画像データを伸張するＪＰＥＧ伸張手段を備え、チェックコードをＪＰＥＧ圧縮データのヘッダーから抽出したので、デジタル画像の改変を簡便な方法で検出でき、悪意を持った第三者の改変を高い信頼性で防止できる。

【００７４】請求項７に記載したチェックコードの生成方法によれば、記録媒体に記録されている画像データが改変されたものであるかどうかを容易に検出でき、しかも解読のされにくいチェックコードを生成できる。

【００７５】請求項８の方法では、サンプリング番号を変数とした暗証番号が、暗号関数に基づいて生成されているので、チェックコードの解析は非常に困難になり、映像データの証拠能力を高めるうえで有効である。

【００７６】請求項９の方法では、チェックコードが、抽出されたサンプリングデータと暗証番号とを変数とする算術加算関数によって生成されているので、少ないサンプリングポイントを使用するだけで、映像データの改変が確実に検出できる。

【００７７】請求項１０の方法では、チェックコードが、抽出されたサンプリングデータと暗証番号とを変数とするガロア体上での加算によって生成されているので、サンプリングデータが異なれば必ず異なるチェックコードが生成され、映像データの改変を見逃してしま

う可能性を小さくすることができる。

【００７８】請求項１１の方法では、チェックコードが、抽出されたサンプリングデータと暗証番号とを変数とする排他的論理和演算によって生成されているので、簡単にチェックコードを生成できる。

【００７９】請求項１２の方法では、サンプリングデータが、圧縮されたデジタルデータの中から暗号関数に基づいて抽出されているので、解読のされにくいチェックコードを生成できる。

【図面の簡単な説明】

【図１】 この発明の実施の形態１に係るデジタル画像記録再生装置の構成を示すブロック図である。

【図２】 この発明の実施の形態１に係る記録動作を示すフローチャートである。

【図３】 この発明の実施の形態１に係る再生動作を示すフローチャートである。

【図４】 この発明の実施の形態１に係るチェックコードの生成を模式的に示す図である。

【図５】 この発明の実施の形態１に係るチェックコードを示す図である。

【図６】 この発明の実施の形態３に係るチェックコードを示す図である。

【図７】 この発明の実施の形態７に係る再生動作を示すフローチャートである。

【図８】 従来のデジタル画像記録再生装置の構成を示すブロック図である。

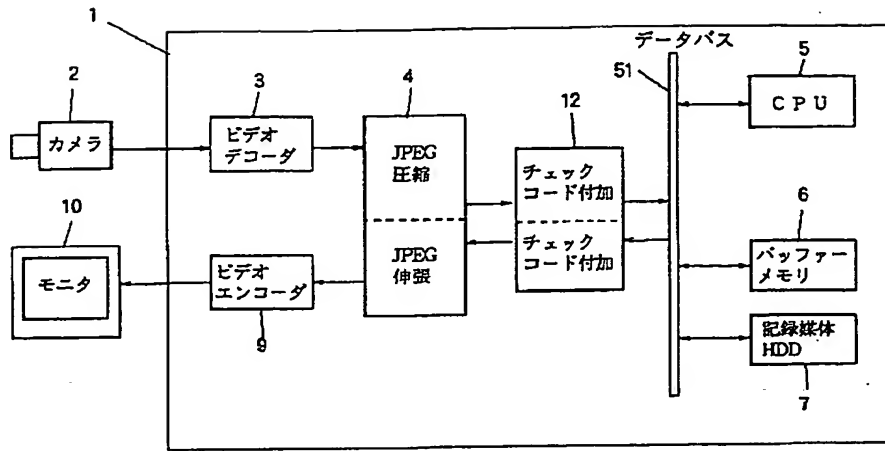
【図９】 従来のデジタル画像記録再生装置の記録動作を示すフローチャートである。

【図１０】 従来のデジタル画像記録再生装置の再生動作を示すフローチャートである。

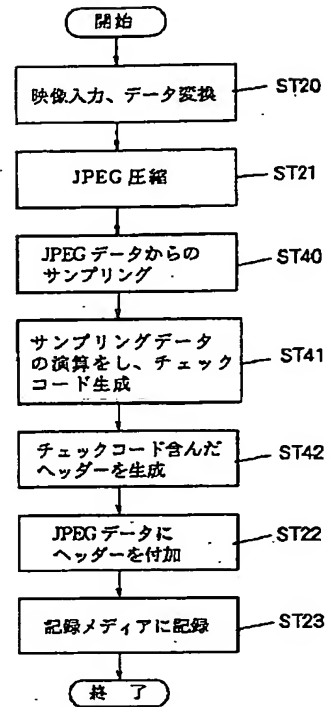
【符号の説明】

１ デジタル画像記録再生装置、２ ビデオカメラ、３ ビデオデコーダ、４ ＪＰＥＧ圧縮伸張手段、５ ＣＰＵ、６ バッファメモリ、７ 記録メディア、８ 通信インターフェース、９ ビデオエンコーダ、１０ モニタテレビ、１２ チェックコード付加解析器、５１ データバス。

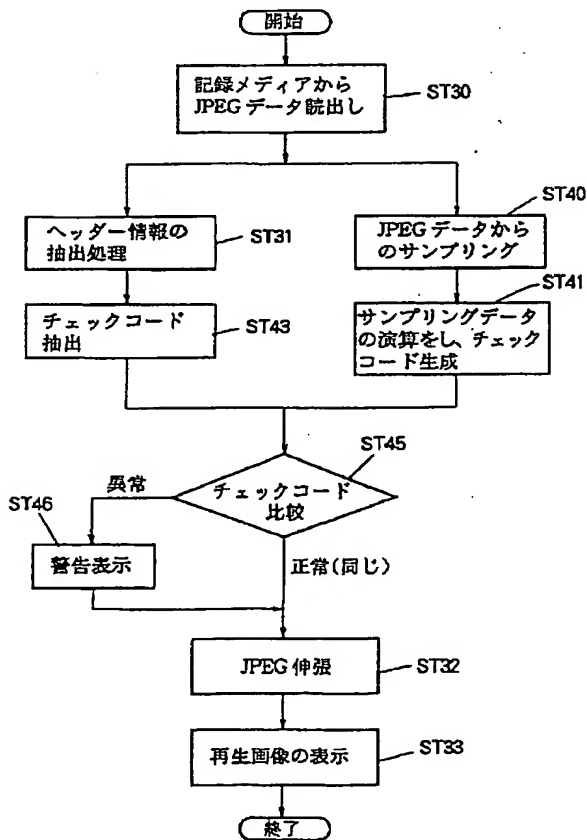
【図 1】



【図 2】



【図 3】

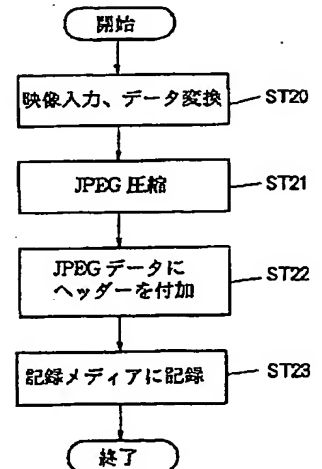


【図 5】

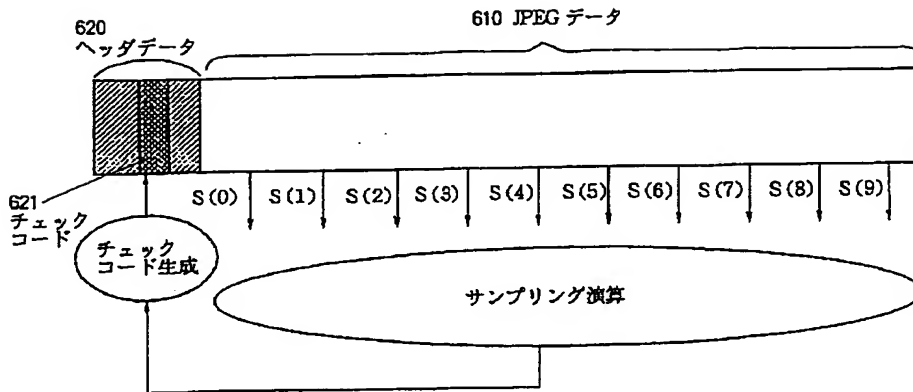
チェックコード

S(0)+0
S(1)+1
S(2)+2
S(3)+3
S(4)+4
S(5)+5
S(6)+6
S(7)+7
S(8)+8
S(9)+9

【図 9】



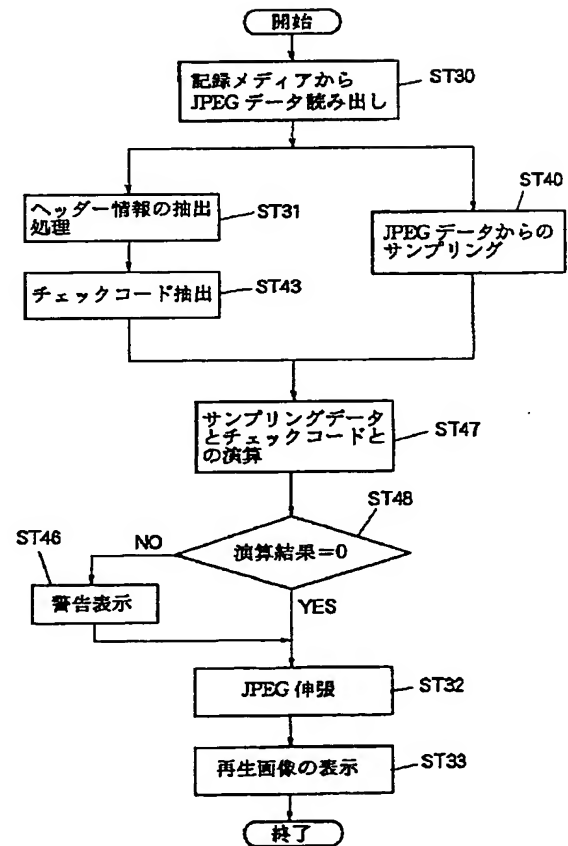
【図 4】



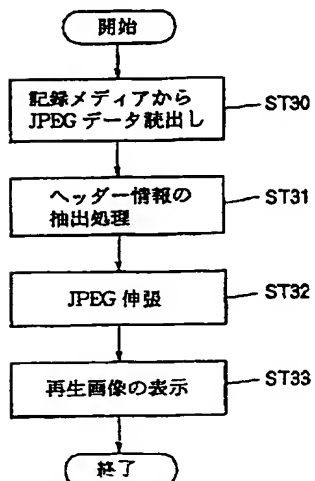
【図 6】



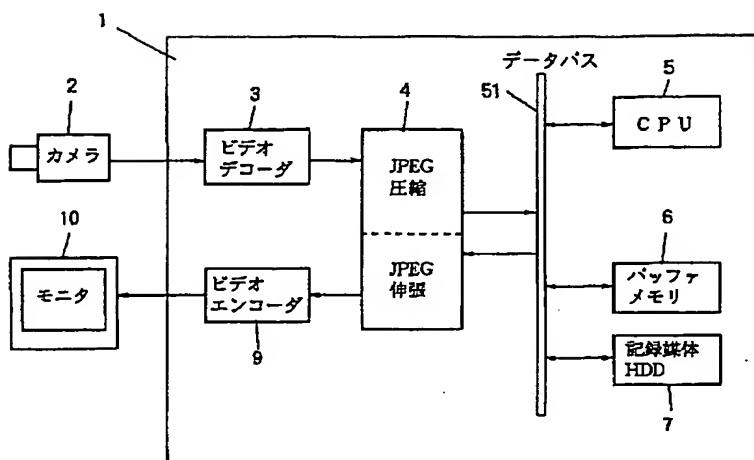
【図 7】



【図 10】



【図 8】



THIS PAGE BLANK (USPTO)